On the properties of the CTR encryption mode of the Magma and Kuznyechik block ciphers with re-keying method based on CryptoPro Key Meshing

Liliya R. Ahmetzyanova[1], Evgeny K. Alekseev[2], Igor B. Oshkin[3], Stanislav V. Smyshlyaev[4], Lolita A. Sonina[5]

Abstract

This paper presents a security bound in the standard security model for the Magma cipher CTR encryption mode and the «CryptoPro Key Meshing» (CPKM) re-keying method that was previously used with the GOST 28147-89 cipher. We enumerate the main requirements that should be followed during the development of re-keying methods, then we propose a modified method and justify its advantages over CPKM . We also obtain certain results about the operational features of the Kuznyechik cipher CTR encryption mode with several re-keying methods.

1 Introduction

The effectiveness of many cryptanalytic methods (see, e.g. [6] and [7]) depends heavily on amount of material (e.g., pairs of plaintext and ciphertext) obtained using a single key. The amount of data that is processed with one key is called a key capacity. The key capacity should be limited in order to prevent the adversary to obtain any significant information, which results in the necessity to use special encryption modes that assume a key transformation every time after a given amount of data is processed.

The introduction of new Magma and Kuznyechik (see [1]) standard block ciphers and their encryption modes (see [2]) in Russia makes it necessary to define some re-keying methods. The re-keying method for the GOST 28147-89 algorithm [8] is defined in [4] and is called «CryptoPro Key Meshing». In the paper [5] the combinatorial and probabilistic properties of this method are analyzed, but there is no analysis of its impact on cryptographic properties of the used encryption mode. As there is an opportunity to use this re-keying method or methods based on it with the new block ciphers it is relevant to analyze the properties of encryption modes which include a re-keying method.

[1]Engineer-Analyst, CryptoPro LLC, lah@cryptopro.ru
[2]Leading engineer-analyst, Crypto-Pro LLC, Ph.D., alekseev@cryptopro.ru
[3]Deputy head of information security department, Crypto-Pro LLC, Ph.D., oshkin@cryptopro.ru
[4]Head of information security department, Crypto-Pro LLC, Ph.D., svs@cryptopro.ru
[5]Engineer-analyst, Crypto-Pro LLC, sonina@cryptopro.ru

In developing a new re-keying method the operational differences between the Magma and Kuznyechik ciphers, such as block size and key extension complexity, should be taken into account. Therefore it is interesting to analyze the influence of the Kuznyechik's features with re-keying method on the efficiency of the extended encryption mode.

2 Notations

By V_n we denote a set of n-component bit vectors. We denote by $M_{(i)}$ the i-th bit, $i \in \{0, \ldots, n-1\}$, of the string $M \in V_n$. For $A \in V_n$ and $B \in V_m$ we denote by $A||B$ a string $A_{(0)}|| \ldots ||A_{(n-1)}||B_{(0)}|| \ldots ||B_{(m-1)} \in V_{n+m}$. Let $|M|$ be a bit length of the string M, and $|M|_8$ – a byte length.

For some set A we will denote by $Perm(A)$ a set of all bijective mappings on A (permutations on A), and by $Func(A)$ — a set of all mappings from A to A. A block cipher E (or just a cipher) is a set of permutations $\{E_K | K \in V_k\} \subseteq Perm(V_n)$, where K is a key. For $M \in V_{mn}$ we denote by M_i, $0 \leqslant i \leqslant m-1$, a string $M_{(i \cdot n)}||M_{(i \cdot n+1)}|| \ldots ||M_{(i \cdot n+n-1)} \in V_n$ and call it the i-th block of the string M. Thus the string M is presented as $M = M_0||M_1|| \ldots ||M_{m-1}$. If $IV \in V_{\frac{n}{2}}$, then we assume that IV_i, $i \in \{0, 1, \ldots, 2^{\frac{n}{2}} - 1\}$, is a string $IV||i \in V_n$, implying without additional notations that IV is concatenated with $n/2$-bit representation of the number i, defined according to [2].

We model an adversary using a probabilistic Turing machine. If an algorithm $\mathcal{A}$ with inputs $X_1, \ldots, X_t$ returns Y as a result, then let $\mathcal{A}(X_1, \ldots, X_t) \Rightarrow Y$. If a value s is chosen from a set S at random according to uniform distribution, then let $s \in_{\mathcal{U}} S$. We suppose that $\mathcal{A}(t, a, b, \ldots)$ is a set of the adversaries whose computational resources (a sum of program size and average complexity) are not greater than t and the other parameters (e.g. a number of requests to oracles) are limited with values $a, b, \ldots$ (the sense of these parameters is explained in each specific case). If $\mathcal{T}$ is a decisional task where an adversary A should distinguish a bit b, then the advantage of this adversary in the $\mathcal{T}$ task is

$$\mathbf{Adv}^{\mathcal{T}}(A) = \Pr[A \Rightarrow 1 | b = 1] - \Pr[A \Rightarrow 1 | b = 0].$$

3 Block ciphers encryption modes

Block cipher is used as a basic function to construct some protocols. The challenge of confidentiality is solved with the use of block cipher in a special way. In this case we indicate «an encryption mode».

In the present paper we consider a CTR encryption mode, defined according to [2] (in case, when $s = n$): the result of the encryption of a message $M = M_0|| \ldots ||M_{m-1}||M_m$, $M_0, \ldots, M_{m-1} \in V_n$, $M_m \in V_r$, is a string $IV||C_0|| \ldots ||C_{m-1}||C_m$, where $IV \in V_{\frac{n}{2}}$,

$C_i = M_i \oplus E_K(IV_i)$ and $C_m = M_m \oplus E_K(IV_m)_{(0)}||\ldots||E_K(IV_m)_{(r-1)}$. In addition, the strings IV are different for different messages processed with one key.

A periodical key transformation for long message processing is considered as an extension of the basic encryption mode. The «CryptoPro Key Meshing» re-keying method for the GOST 28147-89 algorithm [8] is defined in [4] in the following way:

$$K_{i+1} = E^{-1}_{K_i}(D_1)||E^{-1}_{K_i}(D_2)||E^{-1}_{K_i}(D_3)||E^{-1}_{K_i}(D_4),$$

where $D_1, D_2, D_3, D_4 \in V_{64}$ are pairwise different constants.

We consider an incomplete version of the CPKM method, where only the key is changed. There is an additional rule for changing IV in the original CPKM method. For the Kuznyechik cipher we assume an algorithm that is similar to CPKM but uses two 128-bits constants instead of four, and we denote it by CPKM_{128}.

We denote by $\mathrm{CTR\text{-}CPKM}_l$ the CTR encryption mode that assumes the key transformation according to the CPKM method after every l processed blocks of message. The string which consists of message blocks processed using one key is called «a section».

4 The target properties of the perspective re-keying method

The requirements to the re-keying method which is used in high-level cryptographic protocols can be divided into operational and cryptographic. The main operational requirements are:

1. Maximal efficiency in case of short data processing — the first section should be processed using the initial key.
2. Efficiency — the data processing speed with the re-keying method is not much different from the speed without it.

The cryptographic requirements are formulated in the following way:

1. Common security — the use of the re-keying method should improve the security properties of the initial encryption scheme.
2. Security in the extended model — the complexity of one section key disclosure with side channels information should slightly differ from cases where adversary additionally has the same information about keys of other sections.
3. Forward secrecy — the comprometation of the key used in one section should not compromise the keys or data used in previous sections.

These requirements should be followed during the development of re-keying methods with the new standard block ciphers and theirs encryption modes.

In section 6 we give the security bounds of the CTR-CPKM$_l$ encryption mode in the common model, i.e. we analyze whether the CPKM method satisfies the first requirement.

The re-keying methods which are similar to CPKM satisfy the first operational requirement. The second requirement is considered in section 8, where we show certain results about the operational features of the Kuznyechik cipher in the CTR encryption mode with several re-keying method.

5 Known models and security bounds

It is a common practice to bound security of block ciphers in the PRF and PRP-CCA models (see, e.g. [3]), for clarity we call them tasks.

Definition 5.1. *A PRF («Pseudo Random Function») task for a cipher* $\{E_K : V_n \to V_n | K \in V_k\}$ *is the following decisional task. An adversary* A *has access to an oracle* $\mathcal{O}^{PRF}$ *which operates in the following way. Before starting the work the oracle* $\mathcal{O}^{PRF}$ *chooses* $b \in_{\mathcal{U}} \{0,1\}$. *If* $b = 0$, *then* $\mathcal{O}^{PRF}$ *chooses a function* $F \in_{\mathcal{U}} Func(V_n)$ *and if* $b = 1$, *then it chooses a key* $K \in_{\mathcal{U}} V_k$. *The oracle* $\mathcal{O}^{PRF}$ *with input* $M \in V_n$ *returns either* $F(M)$ *(if* $b = 0$*) or* $E_K(M)$ *(if* $b = 1$*).*

The advantage of the cipher E *in the PRF task with parameters* t *and* q *(*q *is a number of queries to the oracle* $\mathcal{O}^{PRF}$*) is*

$$\mathbf{Adv}_E^{PRF}(t,q) = \max_{A \in \mathcal{A}(t,q)} \mathbf{Adv}_E^{PRF}(A).$$

Definition 5.2. *A PRP-CCA («Pseudo Random Permutation in Chosen Ciphertext Attack») task for a cipher* $\{E_K : V_n \to V_n | K \in V_k\}$ *is the following decisional task. An adversary* A *has access to oracles* $\mathcal{O}^{PRP}$ *and* $\mathcal{O}^{PRP^{-1}}$ *which operate in the following way. Before starting the work the oracle* $\mathcal{O}^{PRP}$ *chooses* $b \in_{\mathcal{U}} \{0,1\}$. *If* $b = 0$, *then* $\mathcal{O}^{PRP}$ *chooses a permutation* $R \in_{\mathcal{U}} Perm(V_n)$, *and if* $b = 1$, *then it chooses a key* $K \in_{\mathcal{U}} V_k$. *The oracle* $\mathcal{O}^{PRP}$ *with an input* $M \in V_n$ *returns either* $R(M)$ *(if* $b = 0$*) or* $E_K(M)$ *(if* $b = 1$*). The oracle* $\mathcal{O}^{PRP^{-1}}$ *takes the input string* M *and returns the result of the permutation that is the inverse of the function realized by the oracle* $\mathcal{O}^{PRP}$.

The advantage of the cipher E *in the PRP-CCA task with parameters* t *and* q_1, q_2 *(*q_1 *is a number of queries to the oracle* $\mathcal{O}^{PRP}$, q_2 *is a number of queries to the oracle* $\mathcal{O}^{PRP^{-1}}$*) is*

$$\mathbf{Adv}_E^{PRP\text{-}CCA}(t,q_1,q_2) = \max_{A \in \mathcal{A}(t,q_1,q_2)} \mathbf{Adv}_E^{PRP\text{-}CCA}(A).$$

In case of the block cipher that has no specific methods to decrease the security, the values $\mathbf{Adv}_E^{\mathrm{PRF}}(t,q)$ and $\mathbf{Adv}_E^{\mathrm{PRP\text{-}CCA}}(t,q_1,q_2)$ are bounded considering the characteristics of common methods which solve these tasks. For the PRF task it is a method based on the birthday paradox, and for the PRP-CCA task it is a brute force attack. So for such cipher E we assume the following approximations:

$$\mathbf{Adv}_E^{\text{PRP-CCA}}(t,q) \approx \frac{t}{2^k}, \qquad \mathbf{Adv}_E^{\text{PRF}}(t,q) \approx \frac{t}{2^k} + \frac{q^2}{2^n}. \tag{1}$$

A standard model to bound security of encryption modes is a LOR-CPA task (see, e.g. [3]).

Definition 5.3. *A LOR-CPA («Left Or Right in Chosen Plaintext Attack») task for a $\mathcal{SE}$ encryption mode is the following decisional task. An adversary A has access to an oracle $\mathcal{O}^{LOR}$ that operates in the following way. Before starting the work the oracle $\mathcal{O}^{LOR}$ chooses $b \in_{\mathcal{U}} \{0,1\}$. The adversary A can make requests to the oracle $\mathcal{O}^{LOR}$, each of these requests is a pair of strings (M^0, M^1), where $|M^0| = |M^1|$. In response to the request (M^0, M^1) the oracle returns a string C that is a result of the processing string M^b according to the $\mathcal{SE}$ encryption mode.*

The advantage of the $\mathcal{SE}$ mode in the LOR-CPA task with parameters t, q, m (q is a number of queries to the oracle $\mathcal{O}^{LOR}$, m is a maximal amount of blocks that the messages in query can consist of) is

$$\mathbf{Adv}_{\mathcal{SE}}^{\textit{LOR-CPA}}(t,q,m) = \max_{A \in \mathcal{A}(t,q,m)} \mathbf{Adv}_{\mathcal{SE}}^{\textit{LOR-CPA}}(A).$$

Theorem 5.4. *[3] The following inequality holds*

$$\mathbf{Adv}_{\textit{CTR}}^{\textit{LOR-CPA}}(t,q,m) \leqslant 2 \cdot \mathbf{Adv}_E^{\textit{PRF}}(t + q + nqm, qm).$$

6 Security bound of the CTR-CPKM encryption mode in the LOR-CPA model

The main element of the proof of the theorem on security of the CTR-CPKM$_l$ encryption mode is the introduction of an intermediate IND-KM$_{l,m}$ task, that is used to replace the CTR-CPKM$_l$ mode by the abstract CTR-RK$_l$ mode where a key is chosen at random for every new section.

Definition 6.1. *An IND-KM$_{l,m}$ task, where $l, m \in \mathbb{N}$, for a set of permutations $\mathcal{F} \subset Perm(V_n)$ is the following decisional task. An adversary A has an access to an oracle $\mathcal{O}^{\textit{IND-KM}_{l,m}}$, that stores an initialy empty set $\mathcal{I}$. Before starting the work the oracle $\mathcal{O}^{\textit{IND-KM}_{l,m}}$ chooses bit $b \in_{\mathcal{U}} \{0,1\}$ and a permutation $F \in_{\mathcal{U}} \mathcal{F}$. The first query of the adversary A is a number $j \in \{0, 1, \ldots, m-1\}$. The oracle $\mathcal{O}^{\textit{IND-KM}_{l,m}}$ returns a string $K' = F^{-1}(D_1)||F^{-1}(D_2)||F^{-1}(D_3)||F^{-1}(D_4)$ in response, if $b = 1$, and $K' \in_{\mathcal{U}} V_k$, if $b = 0$. The following queries of the adversary A to the oracle are empty strings. In response to each of these queries the oracle $\mathcal{O}^{\textit{IND-KM}_{l,m}}$ operates as follows: chooses $IV \in_{\mathcal{U}} V_{\frac{n}{2}} \setminus \mathcal{I}$, adds the element IV to $\mathcal{I}$ and returns $IV||F(IV_{j \cdot l})|| \ldots ||F(IV_{j \cdot l + l - 1})$.*

We denote by $\mathbf{Adv}_{\mathcal{F}}^{\textit{IND-KM}_{l,m}}(t,q)$ *the following value:*

$$\mathbf{Adv}_{\mathcal{F}}^{\textit{IND-KM}_{l,m}}(t,q) = \max_{A \in \mathcal{A}(t,q)} \mathbf{Adv}_{\mathcal{F}}^{\textit{IND-KM}_{l,m}}(A).$$

Lemma 6.1. *The following inequality holds*

$$\mathbf{Adv}_{E}^{\textit{IND-KM}_{l,m}}(t,q) \leqslant 2 \cdot \mathbf{Adv}_{E}^{\textit{PRP-CCA}}\left(t + q \cdot \frac{n}{2}, q \cdot l, 4\right) + \frac{8ql+6}{2^n} + \left(\frac{4ql}{2^n}\right)^2.$$

The following final bound holds.

Theorem 6.2. *The inequality holds for natural* l, t, q *and* m *for* $k \in \{4n, 2n\}$

$$\mathbf{Adv}_{\textit{CTR-CPKM}_l}^{\textit{LOR-CPA}}(t,q,ml) \leqslant 4m \cdot \mathbf{Adv}_{E}^{\textit{PRP-CCA}}\left(t + mlq + q \cdot \frac{n}{2}, q \cdot l, \frac{k}{n}\right) + \\ + 2m \cdot \mathbf{Adv}_{E}^{\textit{PRF}}(t + qml, ql) + 2m\delta,$$

where $\delta = \frac{8ql+6}{2^n} + \left(\frac{4ql}{2^n}\right)^2$, *if* $k = 4n$, *and* $\delta = \frac{4ql+1}{2^n} + \left(\frac{2ql}{2^n}\right)^2$, *if* $k = 2n$.

Compare the security bounds of the CTR and CTR-CPKM$_l$ modes in the LOR-CPA model. We assume that for the used cipher E the assumptions (1) hold. If these assumptions hold it can be shown that the obtained bounds for the CTR and CTR-CPKM$_l$ modes are achievable. We also assume that $2^k \gg 2^n$, that holds for the Magma and Kuznyechik ciphers. For convenience we use the value ml instead of m in case of the CTR mode. So amount of processed blocks is at most equal to qml. If $qml < 2^{n/2}$ and $t \ll 2^k$ then for the Magma cipher the following inequalities hold

$$\mathbf{Adv}_{\mathrm{CTR}}^{\mathrm{LOR\text{-}CPA}}(t,q,ml) \approx \frac{2m^2q^2l^2}{2^n} + \frac{t+q+nmql}{2^k} \approx m^2 \cdot \frac{2q^2l^2}{2^n},$$

$$\mathbf{Adv}_{\mathrm{CTR\text{-}CPKM}_l}^{\mathrm{LOR\text{-}CPA}}(t,q,ml) \approx 2m\left(2 \cdot \frac{t+qml}{2^k} + \frac{q^2l^2}{2^n} + \frac{t+qml}{2^k} + \delta\right) \approx m \cdot \frac{2q^2l^2}{2^n}.$$

These relations indicate that the security of the CTR-CPKM$_l$ mode is improved in comparison with the security of the basic CTR mode. The arguments and the final conclusions for the Kuznyechik cipher and the CPKM$_{128}$ re-keying method are similar to the Magma cipher.

7 Open questions

Despite the fact that the CPKM re-keying method improves the security of the CTR encryption mode, this re-keying method has the following properties:

- a key with equal n-bit blocks cannot be a result of the CPKM method;

- if there is a block of gamma that coincides with one of the constants used in the CPKM method then an adversary obtains a part of the key of the next section.

Consider the following method that doesn't have the second property that can be regarded as disadvantage:

$$K' = \mathrm{KM}_l(K) = E_K(\varphi(D_1))||E_K(\varphi(D_2))||E_K(\varphi(D_3))||E_K(\varphi(D_4)),$$

where $\varphi : V_{64} \to V_{64}$, $\varphi(X_1||X||X_2) = X_1||1||X_2$ for $X_1 \in V_{32}$, $X_2 \in V_{31}$, $X \in V_1$ and $D_1, D_2, D_3, D_4 \in V_{64}$ are arbitrary constants such that $\varphi(D_1), \varphi(D_2), \varphi(D_3), \varphi(D_4)$ are pairwise different values. The message size should be less than $2^{n/2-1}$.

The given limitation on a value l, the use of the encryption instead of the decryption and the additional function φ guarantee that blocks encrypted using this method cannot coincide with blocks IV_i. This follows from the fact that for any IV_i the most significant bit of the second semiblock is 0 and the function φ set this value to 1.

A security bound of the CTR-KM mode is obtained in the same way as for the CTR-CPKM mode but there are several differences that support the KM method. The first difference is that in the final bound the value $\mathbf{Adv}_E^{\text{PRP-CCA}}(\cdot,\cdot,\cdot)$ is replaced by $\mathbf{Adv}_E^{\text{PRP-CPA}}(\cdot,\cdot)$. It is known (see, e.g. [3]) that $\mathbf{Adv}_E^{\text{PRP-CPA}}(\cdot,\cdot) \leqslant \mathbf{Adv}_E^{\text{PRP-CCA}}(\cdot,\cdot,\cdot)$, but the capabilities of adversaries in the PRP-CCA model is significantly greater then the capabilities in the PRP-CPA task. If new methods that decrease a cipher security appear it is more likely that $\mathbf{Adv}_E^{\text{PRP-CPA}}(\cdot,\cdot)$ will be strictly less than $\mathbf{Adv}_E^{\text{PRP-CCA}}(\cdot,\cdot,\cdot)$. The second difference is that the value δ in Theorem 6.2 will decrease as the KM method doesn't allow to consider adversaries that use the second property described above in order to solve the IND-$\mathrm{KM}_{l,m}$ task.

Also the KM method has some operational advantages over CPKM. For some ciphers, particularly for Kuznyechik, encryption and decryption code are very different. Therefore it is relevant to use encryption procedure instead of decryption one in the re-keying method in order not to increase the code size.

Note that the KM method has the first combinatorial property described above. This property was analyzed in detail in [5]. It could be regarded as disadvantage but as Theorem 6.2 shows this property doesn't influence on the security in the model with computationally limited adversary.

8 Influence of the Kuznyechik's properties on efficiency of the CTR mode with re-keying method

The use of the re-keying method with any encryption mode decreases data processing speed. We analyze the correlation between encryption efficiency and value l, re-keying method and procedures related to this method. The IV transformation was not made. The measurement was made during the encryption of one long message in the CTR mode. The computer with the following characteristics was used: Intel Core i5-6500 CPU 3.20GHz, L1 D-Cache 32 KB x 4, L1 I-Cache 32 KB x 4, L2 Cache 256 KB x 4.

Speed of the encryption process in the CTR mode in the case where the re-keying method was not used is equal to 335 MB/s. In the tables below the speed is expressed in megabytes per second.

l	1 KB	2 KB	4 KB	8 KB	16 KB	32 KB	64 KB
	320.8	322.5	324.2	325.4	326.5	329.4	330.0

Table 1: A key is not changed, a repeated key extension is not made — slowing is explained by a repeated function call.

l	1 KB	2 KB	4 KB	8 KB	16 KB	32 KB	64 KB
	142.2	197.9	247.3	281.3	302.7	308.9	316.6

Table 2: The key is not changed, but there is the repeated key extension.

The Table 2 shows a contribution of the key extension in the complexity of the key transformation.

l	1 KB	2 KB	4 KB	8 KB	16 KB	32 KB	64 KB
	132.7	186.1	233.4	266.9	287.6	300.0	306.0

Table 3: The CPKM_{128} re-keying method.

l	1 KB	2 KB	4 KB	8 KB	16 KB	32 KB	64 KB
	134.2	192.9	242.6	277.3	300.0	308.6	315.6

Table 4: The KM re-keying method.

9 Conclusion

Results obtained in this paper show that the use of the CPKM method with the CTR mode improves the security properties of the initial encryption mode in the standard security model. We propose a modified method and justify its advantages over the CPKM method. We obtain certain results about the operational features of the Kuznyechik cipher in the CTR encryption mode with several re-keying methods.

10 Acknowledgements

The authors are very grateful to Ekaterina Smyshlyaeva for her valuable comments and suggestions concerning the text of the article.

References

[1] «Information technology. Cryptographic Data Security. Block ciphers», GOST R 34.12-2015, Federal Agency on Technical Regulating and Metrology, 2015.

[2] «Information technology. Cryptographic data security. Modes of operation for block ciphers», GOST R 34.13-2015, Federal Agency on Technical Regulating and Metrology, 2015.

[3] Bellare M., Desai A., Jokipii E., Rogaway P. A concrete security treatment of symmetric encryption. In Proceedings of 38th Annual Symposium on Foundations of Computer Science (FOCS '97), pages 394–403. IEEE, 1997.

[4] Popov V., Kurepkin I., Leontiev S. Additional cryptographic algorithms for use with GOST 28147-89, GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 algorithms. RFC 4357. 2007.

[5] Mironkin V. On some probabilistic characteristics of the «CryptoPro Key Meshing» method. Information Security Problems. Computer Systems. №4, 2015. (In Russian)

[6] Matsui M. Linear Cryptanalysis Method for DES Cipher // Advanced in Cryptology - EUROCRYPT'93. Lect. Notes in Comp. Sci., Springer, 1994. V. 765. P. 386-397.

[7] Biham E., Shamir A. Differential Cryptanalysis of DES-like Cryptosystems // Journal of Cryptology. V. 537. P. 2-21. 1990.

[8] «Cryptographic Protection for Data Processing System», GOST 28147-89, Gosudarstvennyi Standard of USSR, Government Committee of the USSR for Standards, 1989. (In Russian)

11 Appendix

Definition 11.1. *For all $l \in \{1, 2, \ldots, 2^{\frac{n}{2}}\}$ and $m \in \{1, \ldots, 2^{\frac{n}{2}}/l\}$ a LOR-CPA$_{m,l}$ task is a following decisional task. An adversary A has access to an oracle $\mathcal{O}^{LOR_m}$, that operates in the following way. Before start of the work the oracle $\mathcal{O}^{LOR_m}$ chooses $b \in_{\mathcal{U}} \{0,1\}$. The adversary A makes the first request $j \in \{0, 1, 2, \ldots, m-1\}$ to the oracle. This request predicts how a counter IV should be processed. The following requests of the adversary A to the oracle $\mathcal{O}^{LOR_m}$ are the pairs (M^0, M^1), where $|M^0| = |M^1| = ln$. The oracle $\mathcal{O}^{LOR_m}$ returns a string $IV||C$ in response, where $IV \in_{\mathcal{U}} V_{\frac{n}{2}}$, and*

$$C = M_0^b \oplus E_K(IV_{jl})|| \ldots ||M_{l-1}^b \oplus E_K(IV_{jl+l-1}).$$

The advantage of the adversary A in the LOR-CPA$_{m,l}$ task for the CTR mode is

$$\mathbf{Adv}_{CTR}^{LOR\text{-}CPA_{m,l}}(A) = \Pr[A \Rightarrow 1 | b = 1] - \Pr[A \Rightarrow 1 | b = 0].$$

The advantage in the LOR-CPA$_{m,l}$ task with parameters t, q (q is the number of requests to the oracle $\mathcal{O}^{LOR_m}$) is

$$\mathbf{Adv}_{CTR}^{LOR\text{-}CPA_{m,l}}(t,q) = \max_{A \in \mathcal{A}(t,q)} \mathbf{Adv}_{CTR}^{LOR\text{-}CPA_{m,l}}(A).$$

Lemma 11.1. *For all $l \in \{1, 2, \ldots, 2^{\frac{n}{2}}\}$ and $m \in \{1, \ldots, 2^{\frac{n}{2}}\}$ the following inequality holds*

$$\mathbf{Adv}_{CTR}^{LOR\text{-}CPA_{m,l}}(t,q) \leqslant 2 \cdot \mathbf{Adv}_{E}^{PRF}(t, ql).$$

Proof. Let $A \in \mathcal{A}(t,q)$ is an adversary such that $\mathbf{Adv}_{\mathrm{CTR}}^{\mathrm{LOR\text{-}CPA}_{m,l}}(A) = \mathbf{Adv}_{\mathrm{CTR}}^{\mathrm{LOR\text{-}CPA}_{m,l}}(t,q) = \varepsilon$. We will construct an adversary B based on the adversary A who solves the PRF task for the cipher E.

We denote by b a bit that determines the oracle behavior in the PRF task.

The adversary B uses the adversary A as a black box. The adversary B chooses bit $b' \in_{\mathcal{U}} \{0,1\}$ and starts the adversary A. After the first request $j \in \{0, 1, \ldots, m-1\}$ the adversary A sends pairs (M^0, M^1), where $|M^0| = |M^1| = ln$. The adversary B models the oracle $\mathcal{O}^{LOR_m}$ behavior in the following way: chooses $IV \in_{\mathcal{U}} V_{\frac{n}{2}}$, makes l requests to the available for him oracle $\mathcal{O}^{PRF}$ with inputs $IV_{jl}, IV_{jl+1}, \ldots, IV_{jl+l-1}$ and returns to the adversary A the following string:

$$IV||M_0^{b'} \oplus \mathcal{O}^{PRF}(IV_{jl})|| \ldots ||M_{l-1}^{b'} \oplus \mathcal{O}^{PRF}(IV_{jl+l-1}).$$

The adversary A returns as a result a bit a. The adversary B returns 1 as a result of his task, if $b' = a$, and 0, otherwise.

Note that if $b = 1$ for the adversary A the environment, modeled by the adversary B, coincides with the environment of the LOR-CPA$_{m,l}$ task, therefore

$$\Pr[B = 1 | b = 1] = \frac{1}{2} + \frac{\varepsilon}{2}.$$

If $b = 0$ the environment, modeled by the adversary B, coincides with the environment of the ideal cipher, i.e. a case, where the oracle $\mathcal{O}^{LOR_m}$ in response to a request (M^0, M^1) returns a string $IV||C$, where $C \in_{\mathcal{U}} V_{ln}$, therefore

$$\Pr\left[B = 1 | b = 0\right] = \frac{1}{2}.$$

By definition,

$$\mathbf{Adv}_E^{\mathrm{PRF}}(B) = \Pr\left[B = 1 | b = 1\right] - \Pr\left[B = 1 | b = 0\right] = \frac{1}{2} + \frac{\varepsilon}{2} - \frac{1}{2} = \frac{\varepsilon}{2}.$$

Thus, we get

$$\mathbf{Adv}_E^{\mathrm{PRF}}(t, ql) \geqslant \mathbf{Adv}_E^{\mathrm{PRF}}(B) = \frac{1}{2} \cdot \mathbf{Adv}_{\mathrm{CTR}}^{\text{LOR-CPA}_{m,l}}(A).$$

Therefore

$$\mathbf{Adv}_{\mathrm{CTR}}^{\text{LOR-CPA}_{m,l}}(t, q) \leqslant 2 \cdot \mathbf{Adv}_E^{\mathrm{PRF}}(t, ql).$$

□

Lemma 11.2. *For all $l \in \{1, 2, \ldots, 2^{\frac{n}{2}}\}$ and $m \in \{1, \ldots, 2^{\frac{n}{2}}/l\}$ the following inequality holds*

$$\mathbf{Adv}_{CTR-RK_l}^{\text{LOR-CPA}}(t, q, ml) \leqslant m \cdot \mathbf{Adv}_{CTR}^{\text{LOR-CPA}_{m,l}}(t + mlqt_E, q),$$

where t_E is the complexity of computation $E_K(\cdot)$.

Proof. Let $A \in \mathcal{A}(t, q, ml)$ is an adversary such that $\mathbf{Adv}_{\mathrm{CTR}-RK_l}^{\text{LOR-CPA}}(A) = \mathbf{Adv}_{\mathrm{CTR}-RK_l}^{\text{LOR-CPA}}(t, q, ml) = \varepsilon$.

We denote by b a bit that determines the oracle $\mathcal{O}^{LOR}$ behavior in the LOR-CPA task for the $\mathrm{CTR} - RK_l$ mode.

Define a set of the hybrid experiments $Hybrid_{A,j}$ for $j \in \{0, 1, \ldots, m\}$. In the experiment $Hybrid_{A,j}$ the oracle $\mathcal{O}^{LOR}$, that is available for A, is replaced by the oracle $\mathcal{O}_j^{LOR}$, that operates in the following way:

- The oracle $\mathcal{O}_j^{LOR}$ chooses m keys $K_0, K_1, \ldots, K_{m-1} \in_{\mathcal{U}} V_k$ independently of each other;
- In response to a request (M^0, M^1), where $|M^0| = |M^1| = mln$, the oracle chooses $IV \in_{\mathcal{U}} V_{n/2}$ and returns the string

  $$IV||C^{[0]}||\ldots||C^{[m-1]},$$

  where

  $$C^{[i]} = M^b_{i \cdot l} \oplus E_{K_i}(IV_{i \cdot l})||\ldots||M^b_{i \cdot l + l - 1} \oplus E_{K_i}(IV_{i \cdot l + l - 1}),$$

  at that $b = 0$, if $i < j$, and $b = 1$, otherwise, for all $0 \leqslant i \leqslant m - 1$.

The result of any experiment described above is what the adversary A returns as a result. Further we denote by $Hybrid_{A,j} \Rightarrow 1$ an event that occurs if the result of the experiment $Hybrid_{A,j}$ is 1.

Note that for the adversary A the environment of the experiment $Hybrid_{A,0}$ is coincides totally with the environment of the LOR-CPA task if $b = 1$, and the environment of the experiment $Hybrid_{A,m}$ — with the environment of the LOR-CPA task if $b = 0$, i.e. the following inequalities hold:

$$\Pr\left[Hybrid_{A,0} \Rightarrow 1\right] = \Pr\left[A \Rightarrow 1 | b = 1\right],$$

$$\Pr\left[Hybrid_{A,m} \Rightarrow 1\right] = \Pr\left[A \Rightarrow 1 | b = 0\right].$$

Construct an adversary B, that uses A as a black box nd solves the LOR-CPA$_{m,l}$ task. We denote by b' a bit that determines the oracle $\mathcal{O}^{LOR_m}$ behavior in the LOR-CPA$_{m,l}$ task.

The adversary B chooses $j \in_{\mathcal{U}} \{0, \ldots, m-1\}$, keys $K_0, \ldots, K_{j-1}, K_{j+1}, \ldots, K_{m-1} \in_{\mathcal{U}} V_k$ and makes the first request j to the oracle $\mathcal{O}^{LOR_m}$. Receiving a pair (M^0, M^1) from the adversary A the adversary B makes a request $(M^0_{[j]}, M^1_{[j]})$ to his oracle $\mathcal{O}^{LOR_m}$, where $M^b_{[j]}$ is the j-th section of the message M^b, that consists of l blocks. He obtains IV and a ciphertext $C^{[j]}$ in response and returns to the adversary A a string

$$IV||C^{[0]}||\ldots||C^{[j-1]}||C^{[j]}||C^{[j+1]}||\ldots||C^{[m-1]},$$

where

$$C^{[i]} = M^b_{i\cdot l} \oplus E_{K_i}(IV_{i\cdot l})||\ldots||M^b_{i\cdot l+l-1} \oplus E_{K_i}(IV_{i\cdot l+l-1}),$$

at that $b = 0$, if $i < j$, and $b = 1$, if $i > j$.

The adversary B returns as a result what the adversary A retuns.

The following inequalities hold

$$\Pr\left[B = 1 | b' = 1\right] = \frac{1}{m} \sum_{j=0}^{m-1} \Pr\left[Hybrid_{A,j} \Rightarrow 1\right],$$

$$\Pr\left[B = 1 | b' = 0\right] = \frac{1}{m} \sum_{j=0}^{m-1} \Pr\left[Hybrid_{A,j+1} \Rightarrow 1\right].$$

Then for the advantage of the adversary B the following relation holds

$$\begin{aligned}
\mathbf{Adv}^{\text{LOR-CPA}_{m,l}}_{\text{CTR}}(B) &= \Pr\left[B = 1 | b' = 1\right] - \Pr\left[B = 1 | b' = 0\right] = \\
&= \frac{1}{m}\left(\sum_{j=0}^{m-1} \Pr\left[Hybrid_{A,j} \Rightarrow 1\right] - \sum_{j=0}^{m-1} \Pr\left[Hybrid_{A,j+1} \Rightarrow 1\right]\right) = \\
&= \frac{1}{m}\left(\Pr\left[Hybrid_{A,0} \Rightarrow 1\right] - \Pr\left[Hybrid_{A,m} \Rightarrow 1\right]\right) = \\
&= \frac{1}{m}\left(\Pr\left[A \Rightarrow 1 | b = 1\right] - \Pr\left[A \Rightarrow 1 | b = 0\right]\right) = \frac{1}{m} \cdot \varepsilon
\end{aligned}$$

The computational resources of the adversary B can be majorised with the value $t + qmlt_E$, where t_E is the complexity of computation $E_K(\cdot)$.

Thus we have

$$\mathbf{Adv}_{\mathrm{CTR}}^{\text{LOR-CPA}_{m,l}}(t + qmlt_E, q) \geqslant \mathbf{Adv}_{\mathrm{CTR}}^{\text{LOR-CPA}_{m,l}}(B) \geqslant \frac{1}{m} \cdot \mathbf{Adv}_{\mathrm{CTR}-RK_l}^{\text{LOR-CPA}}(A).$$

Therefore

$$\mathbf{Adv}_{\mathrm{CTR}-RK_l}^{\text{LOR-CPA}}(t, q, ml) \leqslant m \cdot \mathbf{Adv}_{\mathrm{CTR}}^{\text{LOR-CPA}_{m,l}}(t + qmlt_E, q).$$

□

Lemma 11.3. *The following inequality holds*

$$\mathbf{Adv}_{CTR-RK_l}^{LOR\text{-}CPA}(t, q, ml) \leqslant 2m \cdot \mathbf{Adv}_E^{PRF}(t + qmlt_E, ql).$$

Proof. Proof of this lemma follows from the statements 11.2 and 11.1. □

Remark 11.2. *In the $IND\text{-}KM_{l,m}$ task for the cipher E before start of the work the oracle $\mathcal{O}^{IND\text{-}KM_{l,m}}$ chooses with bit b a key $K \in V_k$ and uses E_K as a function F.*

Lemma 11.4. *The following inequality holds*

$$\mathbf{Adv}_{Perm\{V_n\}}^{IND\text{-}KM_{l,m}}(t, q) \leqslant \frac{8ql + 6}{2^n} + \left(\frac{4ql}{2^n}\right)^2.$$

Proof. Let $A \in \mathcal{A}(t, q)$ is an adversary, who solves the IND-KM$_{l,m}$ task for a set $Perm\{V_n\}$, some l and m, and is such that $\mathbf{Adv}_{Perm\{V_n\}}^{\text{IND-KM}_{l,m}}(A) = \mathbf{Adv}_{Perm\{V_n\}}^{\text{IND-KM}_{l,m}}(t, q)$.

Let b is a bit that determines the oracle $\mathcal{O}^{\text{IND-KM}_{l,m}}$ behavior. We denote by $RP(\cdot)$ a permutation, that is chosen by the oracle before start of the work and by $\overline{C}$ a set $\{D_1, D_2, D_3, D_4\}$.

By definition,

$$\mathbf{Adv}_{Perm\{V_n\}}^{\text{IND-KM}_{l,m}}(A) = \Pr[A = 1 | b = 1] - \Pr[A = 1 | b = 0].$$

We denote by $\mathcal{N}$ all information that the adversary obtained during attack. The value $\mathcal{N}$ is determined by the following three values: a key $K' \in V_k$, a set $\{IV\} \subset V_{\frac{n}{2}}$ of power q and a set $\{RP(IV)\} \subset V_n$, that consists of ql results of the permutation $RP(\cdot)$ on inputs from $\{IV\}$.

Note that if the value $\mathcal{N} = (\{IV\}, \{RP(IV)\}, K')$ is fixed then the adversary's strategy doesn't depend on bit b, therefore

$$\Pr[A = 1 | b = 1, \mathcal{N}] = \Pr[A = 1 | b = 0, \mathcal{N}] = \Pr[A = 1 | \mathcal{N}].$$

By the law of total probability we have

$$\mathbf{Adv}_{Perm\{V_n\}}^{\text{IND-KM}_{l,m}}(A) = \Pr[A=1|b=1] - \Pr[A=1|b=0] =$$
$$= \sum_{\mathcal{N}} \Pr[A=1|\mathcal{N}] \cdot \Pr[\mathcal{N}|b=1] - \sum_{\mathcal{N}} \Pr[A=1|\mathcal{N}] \cdot \Pr[\mathcal{N}|b=0] =$$
$$= \sum_{\mathcal{N}} \underbrace{\Pr[A=1|\mathcal{N}]}_{\leqslant 1} \cdot (\Pr[\mathcal{N}|b=1] - \Pr[\mathcal{N}|b=0]) \leqslant$$
$$\leqslant \sum_{\mathcal{N}:\Pr[\mathcal{N}|b=1]-\Pr[\mathcal{N}|b=0]>0} (\Pr[\mathcal{N}|b=1] - \Pr[\mathcal{N}|b=0])$$

We denote by p_0 the probability $\Pr[\mathcal{N}|b=0]$. If $b=0$ all components of the value $\mathcal{N}$ are chosen independently of each other, therefore:

$$p^0 = \underbrace{\frac{1}{2^{\frac{n}{2}} \cdot (2^{\frac{n}{2}}-1) \cdot \ldots \cdot (2^{\frac{n}{2}}-q+1)}}_{fix\ \{IV\}} \cdot \underbrace{\frac{(2^n-ql)!}{2^n!}}_{fix\ \{RP(IV)\}} \cdot \underbrace{\frac{1}{2^{4n}}}_{fix\ K'} .$$

Consider the probability $\Pr[\mathcal{N}|b=1]$.
By the law of total probability

$$\Pr[\mathcal{N}=(A,B,Z)|b=1] = \sum_{\{IV\},RP(\cdot)} \Pr_{b=1}[\mathcal{N}=(A,B,Z)|\{IV\},RP(\cdot)] \cdot \underbrace{\Pr[\{IV\},RP(\cdot)]}_{\text{independent of } b} .$$

The following relations hold

$$\Pr[\{IV\},RP(\cdot)] = \frac{1}{2^{\frac{n}{2}} \cdot (2^{\frac{n}{2}}-1) \cdot \ldots \cdot (2^{\frac{n}{2}}-q+1)} \cdot \frac{1}{2^n!} = p^*, \quad \forall\ \{IV\}, RP(\cdot);$$

$$\Pr_{b=1}[\mathcal{N}=(A,B,Z)|\{IV\},RP(\cdot)] = \begin{cases} 1, & \text{if } A=\{IV\},\ RP(A)=B,\ RP(Z)=\overline{C}, \\ 0, & \text{otherwise.} \end{cases}$$

Let (A,B,Z) is «coherent», if there is a permutation $RP(\cdot)$ such that $A = \{IV\},\ RP(A)=B,\ RP(Z)=\overline{C}$.
Then

$$\Pr[\mathcal{N} = (A,B,Z)|b=1] = p^* \cdot \sum_{\{IV\}} \sum_{RP(\cdot)} \Pr_{b=1}[(A,B,Z)|\{IV\}, RP(\cdot)] =$$
$$= p^* \cdot \sum_{RP(\cdot)} \Pr_{b=1}[(A,B,Z)|A, RP(\cdot)] =$$
$$= p^* \cdot \sum_{\substack{RP(\cdot):\ RP(A)=B,\\ RP(Z)=\overline{C}}} 1 =$$
$$= p^* \cdot |\{RP(\cdot):\ RP(A) = B,\ RP(Z) = \overline{C}\}|.$$

Let the set $\{RP(IV)\}$ has a $Prop_i$ property, $0 \leqslant i \leqslant 4$, if the condition $|\{RP(IV)\} \cap \overline{C}| = i$ is satisfied.

Find a power of the set $\{RP(\cdot):\ RP(A) = B,\ RP(Z) = \overline{C}\}$ for all «coherent» (A,B,Z) such that the component B has the $Prop_i$ property for some fixed i. The conditions $\{RP(A) = B,\ RP(Z) = \overline{C}\}$ assume that for the permutation $RP(\cdot)$ we know $ql + (4-i)$ transitions, i.e. pairs of input and output values, therefore

$$|\{RP(\cdot):\ RP(A) = B,\ RP(Z) = \overline{C}\}| = (2^n - (ql + 4 - i))!.$$

We denote by p_i^1 a probability $\Pr[\mathcal{N} = (A,B,Z)|b=1]$ for all «coherent» $\mathcal{N}$ such that the component B has the $Prop_i$ property.

Then

$$p_i^1 = \frac{1}{2^{\frac{n}{2}} \cdot (2^{\frac{n}{2}} - 1) \cdot \ldots \cdot (2^{\frac{n}{2}} - q + 1)} \cdot \frac{(2^n - (ql + 4 - i))!}{2^n!}.$$

Note that the inequality $p_i^1 > p^0$ holds for all i, $0 \leqslant i \leqslant 4$. Indeed,

$$p_i^1 = p^0 \cdot \frac{2^{4n} \cdot (2^n - (ql + 4 - i))!}{(2^n - ql)!} \geqslant p^0 \quad \forall\, 0 \leqslant i \leqslant 4.$$

Divide a set $\mathcal{T} = \{\mathcal{N}\}$ that is a set of all possible values $\mathcal{N}$, into 5 disjoint subsets $\mathcal{T}_0, \mathcal{T}_1, \ldots, \mathcal{T}_4$, where the subset $\mathcal{T}_i$ included all $\mathcal{N} = (\{IV\}, \{RP(IV)\}, K')$ such that the set $\{RP(IV)\}$ has the $Prop_i$ property.

Then

$$\sum_{\mathcal{N}:\Pr[\mathcal{N}|b=1]-\Pr[\mathcal{N}|b=0]>0} \left(\Pr\left[\mathcal{N}|b=1\right]-\Pr\left[\mathcal{N}|b=0\right]\right)=$$

$$=\sum_{i=0}^{4}\sum_{\substack{\mathcal{N}\in\mathcal{T}_i\\ \Pr[\mathcal{N}|b=1]>0}}(p_i^1-p^0)\leqslant$$

$$\leqslant\sum_{i=0}^{4}|\underbrace{\{\mathcal{N}:\mathcal{N}\in\mathcal{T}_i,\ \Pr\left[\mathcal{N}|b=1\right]>0\}}_{\mathcal{B}_i}|\cdot(p_i^1-p^0).$$

Find a power of the set

$$\mathcal{B}_i=\{\mathcal{N}=(A,B,Z):(A,B,Z)\text{ is «coherent» and }B\text{ has the }Prop_i\text{ property}\}.$$

The number of B that has property $Prop_i$

$$\binom{4}{i}\frac{(ql)!}{(ql-i)!}\frac{(2^n-4)!}{(2^n-4-(ql-i))!}.$$

If the set B is fixed then a set $A=\{IV\}$ can be chosen arbitrarily from $V_{\frac{n}{2}}$, and a key Z is determined for blocks that are not in the set B only.

Thus,

$$|\mathcal{B}_i|=\underbrace{\binom{4}{i}\frac{(ql)!}{(ql-i)!}\frac{(2^n-4)!}{(2^n-4-(ql-i))!}}_{fix\ B}\cdot\underbrace{\left(2^{\frac{n}{2}}\cdot(2^{\frac{n}{2}}-1)\cdot\ldots\cdot(2^{\frac{n}{2}}-q+1)\right)}_{fix\ \{IV\}=A}\cdot\underbrace{\frac{(2^n-ql)!}{(2^n-ql-(4-i))!}}_{fix\ Z}.$$

Therefore,

$$\mathbf{Adv}^{\text{IND-KM}_{l,m}}_{Perm\{V_n\}}(A)=\sum_{i=0}^{4}|\mathcal{B}_i|\cdot(p_i^1-p^0)=$$

$$=\sum_{i=0}^{4}\underbrace{\binom{4}{i}\frac{(ql)!}{(ql-i)!}\frac{(2^n-4)!}{2^n!}\cdot\frac{(2^n-ql)!}{(2^n-ql-(4-i))!}}_{a_i}\cdot\underbrace{\left(1-\frac{(2^n-ql)!}{2^{4n}\cdot(2^n-(ql+4-i))!}\right)}_{b_i}=$$

$$=a_0\cdot b_0+a_1\cdot b_1+\sum_{i=2}^{4}a_i\cdot b_i.$$

Bound the value $a_0 \cdot b_0$:

$$a_0 \cdot b_0 \leqslant 1 \cdot \left(1 - \frac{(2^n - ql)\cdot(2^n - ql - 1)\cdot(2^n - ql - 2)\cdot(2^n - ql - 3)}{2^{4n}}\right) \leqslant$$
$$\leqslant \frac{ql}{2^n} + \frac{ql+1}{2^n} + \frac{ql+2}{2^n} + \frac{ql+3}{2^n} = \frac{4ql+6}{2^n}.$$

For $1 \leqslant i \leqslant 4$ we have

$$1 - \frac{1}{2^n} \leqslant b_i \leqslant 1,$$

$$a_i = \binom{4}{i} \frac{(ql)!}{(ql-i)!} \frac{(2^n - ql)\cdot \ldots \cdot (2^n - ql - (4-i) + 1)}{2^n \cdot (2^n - 1)\cdot(2^n - 2)\cdot(2^n - 3)} \leqslant$$
$$\leqslant \frac{1}{i!} \cdot (ql)^i \frac{1}{2^n \cdot (2^n - 1) \cdot \ldots \cdot (2^n - i + 1)} \leqslant \frac{1}{i!} \cdot (ql)^i \cdot \left(\frac{4}{2^n}\right)^i.$$

Then

$$\mathbf{Adv}_{Perm\{V_n\}}^{\text{IND-KM}_{l,m}}(A) \leqslant \frac{4ql+6}{2^n} + \frac{4ql}{2^n} + \sum_{i=2}^{4} \frac{1}{i!} \cdot (ql)^i \cdot \left(\frac{4}{2^n}\right)^i \leqslant$$
$$\leqslant \frac{8ql+6}{2^n} + \left(\frac{4ql}{2^n}\right)^2 \sum_{i=2}^{4} \frac{1}{i!} \leqslant \frac{8ql+6}{2^n} + \left(\frac{4ql}{2^n}\right)^2.$$

□

Lemma 11.5. *The following inequality holds*

$$\mathbf{Adv}_E^{\textit{IND-KM}_{l,m}}(t,q) \leqslant 2 \cdot \mathbf{Adv}_E^{\textit{PRP-CCA}}\left(t + q \cdot \frac{n}{2}, q \cdot l, 4\right) + \frac{8ql+6}{2^n} + \left(\frac{4ql}{2^n}\right)^2.$$

Proof. Let $A \in \mathcal{A}(t,q)$ is an adversary who solves the $\text{IND-KM}_{l,m}$ task for the cipher E, some l and m and is such that $\mathbf{Adv}_E^{\text{IND-KM}_{l,m}}(A) = \mathbf{Adv}_E^{\text{IND-KM}_{l,m}}(t,q)$. We will use this adversary as a black box in order to construct an adversary B that solves the PRP-CCA task.

We denote by b a bit that determines the oracles $\mathcal{O}^{\text{PRP}}$ and $\mathcal{O}^{\text{PRP}^{-1}}$ behavior in the PRP-CCA task.

The adversary B intercepts all queries of the adversary A. Receiving from A the first request $j \in \{0, 1, \ldots, m-1\}$, the adversary B remembers the value j, sets $\mathcal{I} = \emptyset$, chooses a bit $b' \in_{\mathcal{U}} \{0,1\}$ and returns K', obtained according to the CPKM algorithm using the oracle $\mathcal{O}^{\text{PRP}^{-1}}$, if $b' = 1$, and $K' \in_{\mathcal{U}} V_k$, if $b' = 0$. Note that the adversary B makes at most 4 queries to the oracle $\mathcal{O}^{\text{PRP}^{-1}}$.

Next queries from the adversary A are processed in the following way: the adversary B chooses $IV \in_{\mathcal{U}} V_{\frac{n}{2}} \setminus \mathcal{I}$, adds $\mathcal{I} = \mathcal{I} \cup \{IV\}$ and returns a string

$$IV||\mathcal{O}^{\text{PRP}}(IV_{j\cdot l})||\mathcal{O}^{\text{PRP}}(IV_{j\cdot l+1})||\ldots||\mathcal{O}^{\text{PRP}}(IV_{j\cdot l+l-1}).$$

Let the adversary A returns a bit a as a result. The adversary B returns 1, if $a = b'$, and 0, otherwise.

Note that if $b = 1$ for the adversary A the environment modelled by B totally coincides with the environment of the target IND-KM$_{l,m}$ task for the cipher E. If $b = 0$, the modelled environment coincides with the environment of the IND-KM$_{l,m}$ task for a set $Perm\{V_n\}$. For the advantage of the adversary B we have

$$\begin{aligned}
\mathbf{Adv}_E^{\text{PRP-CCA}}(B) &= \Pr[B \Rightarrow 1 | b = 1] - \Pr[B \Rightarrow 1 | b = 0] = \\
&= \Pr[A \Rightarrow b' | b = 1] - \Pr[A \Rightarrow b' | b = 0] = \\
&= \Big(1/2 + 1/2 \cdot \mathbf{Adv}_E^{\text{IND-KM}_{l,m}}(A)\Big) - \Big(1/2 + 1/2 \cdot \mathbf{Adv}_{Perm\{V_n\}}^{\text{IND-KM}_{l,m}}(A)\Big) = \\
&= 1/2 \cdot \mathbf{Adv}_E^{\text{IND-KM}_{l,m}}(A) - 1/2 \cdot \mathbf{Adv}_{Perm\{V_n\}}^{\text{IND-KM}_{l,m}}(A) \geqslant \\
&\geqslant 1/2 \cdot \mathbf{Adv}_E^{\text{IND-KM}_{l,m}}(A) - 1/2 \cdot \mathbf{Adv}_{Perm\{V_n\}}^{\text{IND-KM}_{l,m}}(t, q) = \\
&= 1/2 \cdot \mathbf{Adv}_E^{\text{IND-KM}_{l,m}}(A) - 1/2 \cdot \left(\frac{8ql + 6}{2^n} + \left(\frac{4ql}{2^n}\right)^2\right).
\end{aligned}$$

The adversary A is chosen arbitrarily, therefore

$$\mathbf{Adv}_E^{\text{IND-KM}_{l,m}}(t, q) \leqslant 2 \cdot \mathbf{Adv}_E^{\text{PRP-CCA}}(B) + \frac{8ql + 6}{2^n} + \left(\frac{4ql}{2^n}\right)^2.$$

The adversary B makes at most 4 requests to the oracle $\mathcal{O}^{\text{PRP}^{-1}}$, at most $q \cdot l$ requests to the oracle $\mathcal{O}^{\text{PRP}}$. So his computational resources can be majorised with value $t + q \cdot n/2$ (the adversary B needs to generate q strings $IV \in V_{n/2}$). Thus

$$\mathbf{Adv}_E^{\text{IND-KM}_{l,m}}(t, q) \leqslant 2 \cdot \mathbf{Adv}_E^{\text{PRP-CCA}}\Big(t + q \cdot \frac{n}{2}, q \cdot l, 4\Big) + \frac{8ql + 6}{2^n} + \left(\frac{4ql}{2^n}\right)^2.$$

$\square$

Theorem 11.3. *For natural l, t, q and m, $k = 4n$ the following inequality holds*

$$\begin{aligned}
\mathbf{Adv}_{\textit{CTR-CPKM}_l}^{\textit{LOR-CPA}}(t, q, ml) \leqslant 4m \cdot \mathbf{Adv}_E^{\textit{PRP-CCA}}\Big(t + mlq + q \cdot \frac{n}{2}, q \cdot l, 4\Big) + \\
+ 2m \cdot \mathbf{Adv}_E^{\textit{PRF}}(t + qml, ql) + 2m\delta,
\end{aligned}$$

where $\delta = \frac{8ql+6}{2^n} + \left(\frac{4ql}{2^n}\right)^2$.

Proof. Let $A \in \mathcal{A}(t, q, ml)$ is an adversary who solves the LOR-CPA task for the CTR-CPKM$_l$ encryption mode. We will use this adversary as a black box in order to construct an adversary B that solves the IND-KM$_{l,m}$ task.

We denote by b a bit that determines the oracle $\mathcal{O}^{\text{IND-KM}_{m,l}}$ behavior in the IND-KM$_{l,m}$ task and by b' a bit that determines the oracle $\mathcal{O}^{\text{LOR}}$ behavior in the LOR-CPA task.

Determine a set of the hybrid experiments $\{Hybrid_{A,j}\}$ for the adversary A, where $j \in \{0, 1, \dots, m\}$. In the experiment $Hybrid_{A,j}$ the oracle $\mathcal{O}^{\text{LOR}}$ is replaced in the following way. In response to a request (M^0, M^1) a string $IV||C^{[0]}||\dots||C^{[m-1]}$ is returned, this string is constructed as follows: $IV \in V_{\frac{n}{2}}$, the first j sections of the message $M^{b'}$ are processed with random and independent keys $K_0, \dots, K_{j-1}$, a key for processing of the j-th section is generated at random too, but keys for the next sections are produced from the previous one according to the CPKM algorithm. The result of the experiment $Hybrid_{A,j}$ is 1, if the result of the adversary A is equal to b', and 0, otherwise.

Note that

$$\Pr\left[Hybrid_{A,0} \Rightarrow 1\right] = \frac{1}{2} + \frac{1}{2} \cdot \mathbf{Adv}^{\text{LOR-CPA}}_{\text{CTR-CPKM}_l}(A),$$

$$\Pr\left[Hybrid_{A,m} \Rightarrow 1\right] = \frac{1}{2} + \frac{1}{2} \cdot \mathbf{Adv}^{\text{LOR-CPA}}_{\text{CTR-RK}_l}(A).$$

Construct the adversary B. At the beginning he chooses bit $b' \in_{\mathcal{U}} \{0, 1\}$ and $j \in_{\mathcal{U}} \{0, \dots, m-1\}$, then he makes a request j to the oracle $\mathcal{O}^{\text{IND-KM}_{l,m}}$, receiving a key K' in response.

Then B chooses j keys $K_0, \dots, K_{j-1} \in_{\mathcal{U}} V_k$ independently of each other. Intercepting the request (M^0, M^1) from A, the adversary B makes an empty request to the oracle $\mathcal{O}^{\text{IND-KM}_{l,m}}$ and receives IV and the section of gamma, that is generated with this IV and some secret key K (used by this oracle). Note that the returned section of gamma is generated on the blocks $IV_{j \cdot l}, \dots, IV_{j \cdot l + l - 1}$, i.e. this gamma is appropriate to encrypt the j-th section of processed message $M^{b'}$. So the adversary B uses it to process j-th section of the message $M^{b'}$.

The adversary B processes he first j section of the message $M^{b'}$ using the keys $K_0, \dots, K_{j-1}$ and IV, that is obtained from the $\mathcal{O}^{\text{IND-KM}_{l,m}}$ oracle previously. He processes the $j+1$-the section with a key $K_{j+1} = K'$, and the next sections are processed with keys $K_{j+2}, \dots, K_{m-1}$ such that $K_i = \text{CPKM}(K_{i-1})$. Let the adversary A retuns a bit a as a result. The adversary B returns 1, if $a = b'$, and 0, otherwise.

Note that

$$\Pr\left[B \Rightarrow 1 | b = 1, j\right] = \Pr\left[Hybrid_{A,j} \Rightarrow 1\right],$$

$$\Pr\left[B \Rightarrow 1 | b = 0, j\right] = \Pr\left[Hybrid_{A,j+1} \Rightarrow 1\right].$$

For the advantage $\mathbf{Adv}^{\text{IND-KM}_{l,m}}(B)$ we have

$$\begin{aligned}
\mathbf{Adv}_E^{\text{IND-KM}_{l,m}}(B) &= \Pr\left[B \Rightarrow 1 | b=1\right] - \Pr\left[B \Rightarrow 1 | b=0\right] = \\
&= \sum_{j=0}^{m-1} \Pr\left[B \Rightarrow 1 | b=1, j\right] \cdot \Pr\left[j\right] - \sum_{j=0}^{m-1} \Pr\left[B \Rightarrow 1 | b=0, j\right] \cdot \Pr\left[j\right] = \\
&= \frac{1}{m} \sum_{j=0}^{m-1} \left(\Pr\left[Hybrid_{A,j} \Rightarrow 1\right] - \Pr\left[Hybrid_{A,j+1} \Rightarrow 1\right]\right) = \\
&= \frac{1}{m} \cdot \left(\Pr\left[Hybrid_{A,0} \Rightarrow 1\right] - \Pr\left[Hybrid_{A,m} \Rightarrow 1\right]\right) = \\
&= \frac{1}{2m} \cdot \left(\mathbf{Adv}_{\text{CTR-CPKM}_l}^{\text{LOR-CPA}}(A) - \underbrace{\mathbf{Adv}_{\text{CTR-RK}_l}^{\text{LOR-CPA}}(A)}_{\leqslant 2m \cdot \mathbf{Adv}_E^{\text{PRF}}(t+qmlt_E, ql)}\right) \geqslant \\
&\geqslant \frac{1}{2m} \cdot \left(\mathbf{Adv}_{\text{CTR-CPKM}_l}^{\text{LOR-CPA}}(t,q,ml) - 2m \cdot \mathbf{Adv}_E^{\text{PRF}}(t+qmlt_E, ql)\right).
\end{aligned}$$

Therefore

$$\mathbf{Adv}_{\text{CTR-CPKM}_l}^{\text{LOR-CPA}}(t,q,ml) \leqslant 2m \cdot \mathbf{Adv}_E^{\text{IND-KM}_{l,m}}(B) + 2m \cdot \mathbf{Adv}_E^{\text{PRF}}(t+qmlt_E, ql).$$

Bound the computational resources of the adversary B. The adversary makes $(m-1)lq$ computations of the function E and q requests to the oracle $\mathcal{O}^{\text{IND-KM}_{l,m}}$.

Therefore, by the lemma 11.5,

$$\begin{aligned}
\mathbf{Adv}_E^{\text{IND-KM}_{l,m}}(B) &\leqslant \mathbf{Adv}_E^{\text{IND-KM}_{l,m}}(t+mlqt_E, q) \leqslant \\
&\leqslant 2 \cdot \mathbf{Adv}_E^{\text{PRP-CCA}}\left(t+mlqt_E + q \cdot \frac{n}{2}, q \cdot l, 4\right) + \frac{8ql+6}{2^n} + \left(\frac{4ql}{2^n}\right)^2.
\end{aligned}$$

Thus,

$$\begin{aligned}
\mathbf{Adv}_{\text{CTR-CPKM}_l}^{\text{LOR-CPA}}(t,q,ml) &\leqslant 4m \cdot \mathbf{Adv}_E^{\text{PRP-CCA}}\left(t+mlqt_E + q \cdot \frac{n}{2}, q \cdot l, 4\right) + \\
&+ 2m \cdot \mathbf{Adv}_E^{\text{PRF}}(t+qmlt_E, ql) + 2m \cdot \left(\frac{8ql+6}{2^n} + \left(\frac{4ql}{2^n}\right)^2\right).
\end{aligned}$$

□

Remark 11.4. *For a case $k = 2n$ all tasks are formulated similarly, the corresponding theorems are proved in the same way.*

Remark 11.5. *Here we prove that the bounds for the basic CTR encryption mode and for the extended version with the $CPKM$ re-keying methods are achievable.*

Consider an adversary A in the $LOR\text{-}CPA$ task for the CTR encryption mode whose advantage is approximately equal to the bound.

Let the adversary sends to an oracle $\mathcal{O}^{LOR\text{-}CPA}$ q couples (M_i^0, M_i^1), where $M_i^0, M_i^1 \in_R V_{mln}$. The oracle returns ciphertexts C_i, $1 \leqslant i \leqslant q$. The adversary computes a set $G = \{M_i^0 \oplus C_i\}_{1 \leqslant i \leqslant q}$ which consists of qml blocks. If there are two equal blocks in G (denote this event by B) the adversary returns 1. Notice that for the correct plaintext the probability to obtain two equal blocks in G is 0. If all blocks in G are pairwise different the adversary returns a random bit according to uniform distribution.

The probability that there are two equal values among qml realization of a random variable uniformly distributed over a set of power 2^n is approximately equal to $\frac{(qml)^2}{2^{n+1}}$ (birthday paradox).

The following relation holds:

$$\begin{aligned}\mathbf{Adv}_{CTR}^{LOR\text{-}CPA}(A) &= 2 \cdot \Pr[A \Rightarrow b] - 1 = \\ &= 2\Big(\underbrace{\Pr[A \Rightarrow b|\ B]}_{=1} \cdot \Pr[B] + \underbrace{\Pr\left[A \Rightarrow b|\ \overline{B}\right]}_{=\frac{1}{2}} \cdot (1 - \Pr[B])\Big) - 1 = \\ &= \Pr[B] \approx \frac{(qml)^2}{2 \cdot 2^n},\end{aligned}$$

where b is a bit which determines the oracle behavior.

Consider an adversary A' in the $LOR\text{-}CPA$ task for the $CTR\text{-}CPKM_l$ encryption mode whose advantage is approximately equal to the obtained bound. This adversary operates in the same way as A operates except the step of computing the set G. Instead he computes m sets G_i, each of them consists of ql blocks (different sets corresponds to different keys). If there are two equal blocks in G_i for some $1 \leqslant i \leqslant m$ (denote this event by B') the adversary returns 1. If all blocks in G_i for all $1 \leqslant i \leqslant m$ are pairwise different the adversary returns a random bit according to uniform distribution.

Notice that

$$\Pr[B'] \approx 1 - \left(1 - \frac{(ql)^2}{2 \cdot 2^n}\right)^m \approx m \cdot \frac{(ql)^2}{2 \cdot 2^n}$$

Therefore,

$$\mathbf{Adv}_{CTR\text{-}CPKM_l}^{LOR\text{-}CPA}(A') = 2 \cdot \Pr[A' \Rightarrow b] - 1 = \Pr[B'] \approx m \cdot \frac{(ql)^2}{2 \cdot 2^n}.$$